THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE Retreat Behavioral Health LLC	Lead Case No.: 5:23-cv-00026-MRP **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs James Worton and Lauren Small ("Plaintiffs") bring this Class Action Complaint against Retreat at Lancaster County PA LLC ("Retreat Lancaster") and Retreat Behavioral Health LLC ("RBH") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personal identifiable information ("PII")[1] and protected health information ("PHI") (collectively, "Private Information") for individuals who received services from Defendants or their subsidiaries or affiliates, including, but not limited to, first and last name, address, Social Security number, date of birth, and medical and treatment information.

2. RBH, directly and/or through its subsidiaries or affiliates, provides behavioral and mental health services in Florida (4 locations), Pennsylvania (5 locations), and Connecticut (1 location).

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. Retreat Lancaster is one of RBH's subsidiaries or affiliates and provides services in Lancaster County, Pennsylvania.

4. Prior to and through July 1, 2021, RBH, directly or through its subsidiaries or affiliates, obtained the PII and PHI of Plaintiffs and Class Members and stored that PII and PHI, unencrypted, in an Internet-accessible environment on Defendants' network.

5. Defendants represent in their Company Privacy Policy that they implement "reasonable safeguards to prevent or limit … inadvertent disclosures" of PII and PHI.[2]

6. On or before July 1, 2022, Defendants learned that an unauthorized third party accessed Defendants' computer systems during a ransomware attack (the "Data Breach").

7. Defendants determined that the unauthorized actor may have accessed a data set containing the PII and PHI of Plaintiffs and Class Members.

8. On or around December 30, 2022, Defendants began notifying various states Attorneys General of the Data Breach.

9. On or around December 30, 2022, Defendants began notifying Plaintiffs and Class Members of the Data Breach.

10. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admits that the unencrypted PII and PHI exposed to "unauthorized activity" included first and last name, address, Social Security number, date of birth, and medical and treatment information.

11. The exposed PII and PHI of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to

[2] *See* https://www.retreatbehavioralhealth.com/privacy-policy/ (last visited Jan. 3, 2023).

criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their confidential medical information.

12. The PII and PHI were compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members. In addition to Defendants' failure to prevent the Data Breach, Defendants waited several months after the Data Breach occurred to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

13. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their confidential medical information. The risk will remain for their respective lifetimes.

14. Plaintiffs bring this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

15. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud,

and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, including medical information, and (v) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

16. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

17. Plaintiff James Worton is a Citizen of Maryland residing in Rising Sun, Maryland.

18. Plaintiff Small is and has been, at all relevant times, a resident and citizen of New Jersey, currently residing in Verona, New Jersey. Ms. Small received the Notice Letter, via U.S. mail, directly from Defendant, dated December 30, 2022. Ms. Small provided her Private Information to RBH on the condition that it be maintained as confidential and with the understanding that RBH would employ reasonable safeguards to protect her Private Information.

If Ms. Small had known that RBH would not adequately protect her Private Information, she would not have entrusted RBH with her Private Information or allowed RBH to maintain this sensitive Private Information.

19. RBH is a limited liability company organized under the laws of Florida with a principal place of business in Lake Worth, Florida.

20. Retreat Lancaster is a limited liability company organized under the laws of Pennsylvania with a principal place of business in Ephrata, Pennsylvania.

21. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

22. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

23. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendants to establish minimal diversity.

24. Under 28 U.S.C. § 1332(d)(10), RBH is a citizen of Florida because it is a limited liability company formed under Florida law with its principal place of business in Lake Worth, Florida.

25. Under 28 U.S.C. § 1332(d)(10), Retreat Lancaster is a citizen of Pennsylvania because it is a limited liability company formed under Pennsylvania law with its principal place of business in Ephrata, Pennsylvania.

26. The Eastern District of Pennsylvania has personal jurisdiction over Retreat Lancaster because it conducts substantial business in Florida and this District.

27. The Eastern District of Pennsylvania has personal jurisdiction over RBH because it collects PII and PHI from Retreat Lancaster about individuals who obtain services from Retreat Lancaster. RBH also collects data from at least four other subsidiaries or affiliates in Akron, Lansdale, and Philadelphia, Pennsylvania. RBH also sent notices of the Data Breach to residents of Pennsylvania and this District whose PII and PHI was removed during the Data Breach.

28. Venue is proper in this District under 28 U.S.C. §1391(b) because Retreat Lancaster operates in this District, Plaintiff Worton provided and entrusted his PII and PHI to Retreat Lancaster in this District, RBH obtained that PII and PHI from Retreat Lancaster in this District, RBH sent notice of the Data Breach to Plaintiffs and others in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

29. Plaintiffs and Class Members, who obtained services from Defendants or their subsidiaries or affiliates, provided and entrusted Defendants with sensitive and confidential information, including first and last name, address, Social Security number, date of birth, and medical and treatment information.

30. Plaintiffs and Class Members relied on these sophisticated Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes

only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII and PHI.

31. Defendants had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

32. On or about December 30, 2022, RBH sent Plaintiffs and Class Members a notice of the Data Breach (the "Notice of Data Breach").[3] RBH informed Plaintiffs and other Class Members that:

> Retreat Behavioral Health ("RBH") is an addiction treatment center with locations in Florida, Pennsylvania, and Connecticut. We are writing to inform you of an incident that involved your personal information. We take the security of your personal information seriously, and want to provide you with information and resources you can use to protect your information.
>
> What Happened and What Information was Involved:
>
> On July 1, 2022, we detected and stopped a ransomware attack, in which an unauthorized third party accessed some of RBH's computer systems. We immediately engaged a third-party forensic firm to assist us with securing the network environment and investigating the extent of any unauthorized activity. That investigation identified a data set that may have been accessed by the unauthorized person. RBH then performed an extensive and comprehensive review of the data set and identified individuals whose personal information was in that data set. That investigation concluded on December 9, 2022.
>
> We found no evidence that your information has been specifically misused; however, it is possible that the following personal information could have been accessed by an unauthorized third party: first and last name, address, Social Security number, and, in some cases, date of birth and medical and treatment information. Please be assured that your financial account or payment card

[3] Exhibit 1 (sample notice filed with Massachusetts attorney general's office), *available at* https://www.mass.gov/doc/assigned-data-breach-number-28814-retreat-behavioral-health/download (last visited Jan. 3, 2023).

information **were not** compromised as a result of this incident.[4]

33. On or about December 30, 2022, RBH notified various state Attorneys General of the Data Breach and provided them "sample" notices of the Data Breach.

34. Defendants admitted in the Notice of Data Breach, the letters to the Attorneys General, and the "sample" notices of the Data Breach that an unauthorized actor may have accessed a data set containing the PII and PHI of Plaintiffs and Class Members, including first and last name, address, Social Security number, date of birth, and medical and treatment information.

35. In response to the Data Breach, Defendants claim that "[u]pon detecting this incident, we moved quickly to initiate a response, which included retaining a leading forensic investigation firm who assisted in conducting an investigation along with the assistance of leading IT specialists to confirm the security of our network environment. Additionally, we are coordinating with the FBI. We have also deployed additional monitoring tools and will continue to enhance the security of our systems."[5]

36. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

37. The unencrypted PII and PHI of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiffs and Class Members.

---

[4] *Id.*
[5] *Id.*

38. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII and PHI for Plaintiffs and Class Members.

39. Because Defendants had a duty to protect Plaintiffs' and Class Members' PII and PHI, Defendants should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

40. In the years immediately preceding the Data Breach, Defendants knew or should have known that Defendants' computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

41. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ***ransomware actors have also targeted health care organizations***, ***industrial companies***, and the transportation sector."[6]

42. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate

[6] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

negative news for companies as revenge against those who refuse to pay."[7]

43. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[8]

44. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) ransomware actors were targeting healthcare companies such as Defendants, (ii) ransomware gangs were ferociously aggressive in their pursuit of big companies such as Defendants, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

45. In light of the information readily available and accessible on the internet before the Data Breach, Defendants, having elected to store the unencrypted PII and PHI of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and PHI and Defendants' type of business had cause to be particularly on guard against such an attack.

46. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII and PHI could be accessed, exfiltrated,

---

[7] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

[8] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

and published as the result of a cyberattack.

47. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII and PHI to protect against their publication and misuse in the event of a cyberattack.

Defendants Acquire, Collect, and Store the PII and PHI of Plaintiffs and Class Members.

48. As a condition of obtaining services from Defendants, Defendants required that Plaintiffs and Class Members entrust Defendants with highly confidential PII and PHI.

49. Defendants acquired, collected, and stored the PII and PHI of Plaintiffs and Class Members.

50. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

51. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

52. Defendants could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable business need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

53. Defendants' negligence in safeguarding the PII and PHI of Plaintiffs and Class

Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

54. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

55. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[10]

56. The ramifications of Defendants' failure to keep secure the PII and PHI of Plaintiffs and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

57. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to

[9] 17 C.F.R. § 248.201 (2013).

[10] *Id*.

$200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

58. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

59. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

---

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2022).

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

[14] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2022).

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

60. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

61. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license or state identification number, and biometrics.

62. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

63. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

64. The fraudulent activity resulting from the Data Breach may not come to light for

---

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2022).

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

years.

65. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

66. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

67. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

68. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in Defendants' folders and files, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

69. To date, Defendants have offered Plaintiffs and Class Members only two years of single-bureau credit monitoring services. The offered service is inadequate to protect Plaintiffs and

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

70. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class Members.

Plaintiff Worton's Experience

71. In or around 2017, Plaintiff Worton obtained services from Retreat Lancaster. As a condition of providing services to Plaintiff, Retreat Lancaster required that he provide and entrust his PII and PHI.

72. Plaintiff Worton received Defendants' Notice of Data Breach, dated December 30, 2022, on or about that date. The notice stated that Plaintiff Worton's first and last name, address, Social Security number, date of birth, and medical and treatment information were in the data set that the unauthorized actor may have accessed during the Data Breach.

73. As a result of the Data Breach, Plaintiff Worton's PII and PHI may have been accessed by an unauthorized actor. The confidentiality of Plaintiff Worton's PII and PHI has been irreparably harmed. For the rest of his life, Plaintiff Worton will have to worry about when and how his PII and PHI may be shared or used to his detriment.

74. As a result of the Data Breach notice, Plaintiff Worton spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach. This time has been lost forever and cannot be recaptured.

75. Additionally, Plaintiff Worton is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

76. Plaintiff Worton stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

77. Plaintiff Worton suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

78. Plaintiff Worton has suffered imminent and impending injury arising from the substantially increased risk misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

79. Plaintiff Worton has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

80. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

81. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII and/or PHI was accessed or potentially accessed in the data breach that is the subject of the notice that Defendants sent to Plaintiffs and Class Members on or around December 30, 2022 (the "Nationwide Class").

82. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Worton asserts claims on behalf of a separate subclass, defined as follows:

> All individuals who obtained services from Retreat Lancaster and whose PII and/or PHI was accessed or potentially accessed in the data breach that is the subject of the notice that Defendants sent to

> Plaintiffs and Class Members on or around December 30, 2022 (the "Lancaster Subclass").

83. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

> All residents of Pennsylvania who obtained services from RBH and whose PII and/or PHI was accessed or potentially accessed in the data breach that is the subject of the notice that Defendants sent to Plaintiffs and Class Members on or around December 30, 2022 (the "Pennsylvania Subclass").

84. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

85. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

86. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendants operate mental health and behavioral health treatment centers in at least ten locations in three states, reported to the Maine Attorney General that the Data Breach impacted 23,620 individuals, and the Class is apparently identifiable within Defendants' records.

87. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII and PHI of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of

Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

88. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendants' misfeasance.

89. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

90. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

91. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the

controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

92. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

93. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

94. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

95. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII and PHI of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

96. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

97. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

98. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

99. As a condition of obtaining services from Defendants or their subsidiaries or affiliates, Plaintiffs and Nationwide Class Members were obligated to provide and entrust Defendants or their subsidiaries or affiliates with certain PII and PHI.

100. Plaintiffs and the Nationwide Class provided and entrusted their PII and PHI to Defendants or their subsidiaries or affiliates on the premise and with the understanding that Defendants would safeguard their information, use their PII and PHI for business purposes only, and not disclose their PII and PHI to unauthorized third parties.

101. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

102. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

103. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiffs and the Nationwide Class in Defendants' possession was adequately secured and protected.

104. Defendants also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII and PHI they were no longer required to retain pursuant to regulations and had no reasonable business need to maintain in an Internet-accessible environment.

105. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and the Nationwide Class.

106. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendants with their confidential PII and PHI, a necessary part of obtaining services from Defendants or their subsidiaries or affiliates.

107. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

108. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the

Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

109. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendants' systems.

110. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendants.

111. Plaintiffs and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

112. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

113. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiffs and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties and (ii) prepare for the sharing and detrimental use of their confidential medical

information.

114. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiffs and the Nationwide Class.

115. Defendants have admitted that the PII and PHI of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

116. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and the Nationwide Class during the time the PII and PHI was within Defendants' possession or control.

117. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

118. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

119. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII and PHI.

120. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII and PHI they were no longer required to retain pursuant to regulations and which Defendants had no reasonable need to maintain in an Internet-accessible environment.

121. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

122. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII and PHI of Plaintiffs and the Nationwide Class would not have been compromised.

123. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and PHI of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII and PHI of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

124. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate

measures to protect the PII and PHI of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

125. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

126. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

127. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class and Against RBH)

128. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

129. Defendants represent in their Company Privacy Policy that they implement "reasonable safeguards to prevent or limit … inadvertent disclosures" of PII and PHI.

130. In obtaining services from RBH or its subsidiaries or affiliates, Plaintiffs and Nationwide Class Members provided and entrusted their PII and PHI to RBH.

131. Defendants' Company Privacy Policy confirms that RBH intended to bind itself to protect the PII and PHI that Plaintiffs and Nationwide Class Members submitted to RBH or its subsidiaries or affiliates to obtain services.

132. RBH or its affiliates or subsidiaries required Plaintiffs and Nationwide Class Members to provide and entrust their PII and PHI as condition of obtaining services from RBH or its subsidiaries or affiliates.

133. As a condition of obtaining services from RBH or its subsidiaries or affiliates, Plaintiffs and Nationwide Class Members provided and entrusted their PII and PHI. In so doing, Plaintiffs and Nationwide Class Members entered into implied contracts with RBH by which RBH agreed to safeguard and protect such PII and PHI, to keep such PII and PHI secure and confidential, and to timely and accurately notify Plaintiffs and Nationwide Class Members if their PII and PHI had been compromised or stolen.

134. Plaintiffs and the Nationwide Class Members fully performed their obligations under the implied contracts with RBH.

135. RBH breached the implied contracts it made with Plaintiffs and Nationwide Class Members by failing to implement appropriate technical and organizational security measures designed to protect their PII and PHI against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and PHI and by failing to provide timely and accurate notice to them that PII and PHI was compromised as a result of the data breach.

136. As a direct and proximate result of RBH's above-described breach of implied contract, Plaintiffs and Nationwide Class Members have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential medical information; ongoing,

imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

137. As a direct and proximate result of RBH's above-described breach of implied contract, Plaintiffs and Nationwide Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff Worton and the Lancaster Subclass Against Retreat Lancaster)

138. Plaintiff Worton re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 97.

139. Defendants represent in their Company Privacy Policy that they implement "reasonable safeguards to prevent or limit … inadvertent disclosures" of PII and PHI.

140. In obtaining services from Retreat Lancaster, Plaintiff Worton and Lancaster Subclass Members provided and entrusted their PII and PHI to Retreat Lancaster.

141. Defendants' website confirms that Retreat Lancaster intended to bind itself to protect the PII and PHI that Plaintiff Worton and Lancaster Subclass Members submitted to Retreat Lancaster to obtain services.

142. Retreat Lancaster required Plaintiff Worton and Lancaster Subclass Members to provide and entrust their PII and PHI as condition of obtaining services from Retreat Lancaster.

143. As a condition of obtaining services from Retreat Lancaster, Plaintiff Worton and Lancaster Subclass Members provided and entrusted their PII and PHI. In so doing, Plaintiff Worton and Lancaster Subclass Members entered into implied contracts with Retreat Lancaster by which Retreat Lancaster agreed to safeguard and protect such PII and PHI, to keep such PII and PHI secure and confidential, and to timely and accurately notify Plaintiff Worton and Lancaster Subclass Members if their PII and PHI had been compromised or stolen.

144. Plaintiff Worton and Lancaster Subclass Members fully performed their obligations under the implied contracts with Retreat Lancaster.

145. Retreat Lancaster breached the implied contracts it made with Plaintiff Worton and Lancaster Subclass Members by failing to implement appropriate technical and organizational security measures designed to protect their PII and PHI against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and PHI and by failing to provide timely and accurate notice to them that PII and PHI was compromised as a result of the data breach.

146. As a direct and proximate result of Retreat Lancaster's above-described breach of implied contract, Plaintiff Worton and Lancaster Subclass Members have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential medical information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card

statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

147. As a direct and proximate result of Retreat Lancaster's above-described breach of implied contract, Plaintiff Worton and Lancaster Subclass Members are entitled to recover actual, consequential, and nominal damages.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class and Against RBH)

148. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

149. A relationship existed between Plaintiffs and the Nationwide Class and RBH in which Plaintiffs and the Nationwide Class put their trust in RBH to protect the private information of Plaintiffs and the Nationwide Class and RBH accepted that trust.

150. RBH breached the fiduciary duty that it owed to Plaintiffs and the Nationwide Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiffs and the Nationwide Class.

151. RBH's breach of fiduciary duty was a legal cause of damage to Plaintiffs and the Nationwide Class.

152. But for RBH's breach of fiduciary duty, the damage to Plaintiffs and the Nationwide Class would not have occurred.

153. RBH's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and the Nationwide Class.

154. As a direct and proximate result of RBH's breach of fiduciary duty, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff Worton and the Lancaster Subclass and Against Retreat Lancaster)

155. Plaintiff Worton re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

156. A relationship existed between Plaintiff Worton and the Lancaster Subclass and Retreat Lancaster in which Plaintiff Worton and the Lancaster Subclass put their trust in Retreat Lancaster to protect the private information of Plaintiff Worton and the Lancaster Subclass and Retreat Lancaster accepted that trust.

157. Retreat Lancaster breached the fiduciary duty that it owed to Plaintiff Worton and the Lancaster Subclass by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff Worton and the Retreat Lancaster Subclass.

158. Retreat Lancaster's breach of fiduciary duty was a legal cause of damage to Plaintiff Worton and the Lancaster Subclass.

159. But for Retreat Lancaster's breach of fiduciary duty, the damage to Plaintiff Worton and the Lancaster Subclass would not have occurred.

160. Retreat Lancaster's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff Worton and the Lancaster Subclass.

161. As a direct and proximate result of Retreat Lancaster's breach of fiduciary duty, Plaintiff Worton and the Lancaster Subclass are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT VI
VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
(On Behalf of Plaintiffs and the Nationwide Class and Against RBH)

162. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

163. This cause of action is brought pursuant the FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

164. RBH's offer, provision, and/or sale of services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-501.213.

165. Plaintiffs and the Nationwide Class, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

166. RBH provided services to Plaintiffs and the Nationwide Class.

167. RBH offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

168. Plaintiffs and the Nationwide Class paid for or otherwise availed themselves and received services from RBH, primarily for personal, family, or household purposes.

169. RBH engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of employment or services to or from Plaintiffs and the Nationwide Class.

170. RBH's acts, practices, and omissions were done in the course of RBH's businesses of offering, providing, and servicing customers throughout Florida and the United States.

171. The unfair, unconscionable, and unlawful acts and practices of RBH alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

172. RBH, headquartered and operating in and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that their computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiffs' and the Nationwide Class's PII;

d. continued acceptance and storage of PII after RBH knew or should have known of the security vulnerabilities that were exploited in the Data Breach;

e. continued acceptance and storage of PII after RBH knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

173. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 41, *et seq.*, and the FDUTPA, Fla. Stat. § 501.171(2).

174. RBH knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and the Nationwide Class's PII and that the risk of a data breach or theft was high.

175. Plaintiffs have standing to pursue this claim because as a direct and proximate result of RBH's violations of the FDUTPA, Plaintiffs and the Nationwide Class have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that RBH's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

176. Plaintiffs also have standing to pursue this claim because, as a direct result of RBH's knowing violation of the FDUTPA, Plaintiffs are at a substantial present and imminent risk of identity theft. RBH still possesses Plaintiffs' and the Nationwide Class's PII, and Plaintiffs' PII has been potentially accessed by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiffs and the Nationwide Class.

177. Plaintiffs and the Nationwide Class are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that RBH engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on RBH's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that RBH engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that RBH audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that RBH segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that RBH purge, delete, and destroy PII not necessary for its provisions of services in a reasonably secure manner;

f. ordering that RBH conduct regular database scans and security checks;

g. ordering that RBH routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering RBH to meaningfully educate individuals about the threats they face as a result of the loss of their financial and PII to third parties, as well as the steps victims should take to protect themselves.

178. Plaintiffs bring this action on behalf of themselves and the Nationwide Class for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow employees and consumers to make informed purchasing decisions and to protect Plaintiff, the Nationwide Class, and the public from RBH's unfair methods of competition and unfair, unconscionable, and unlawful practices. RBH's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

179. The above unfair, unconscionable, and unlawful practices and acts by RBH were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the Nationwide Class that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

180. RBH's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

181. Plaintiffs and the Nationwide Class seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, a declaratory judgment that RBH's actions and/or practices violate the FDUTPA.

182. Plaintiffs and the Nationwide Class are also entitled to recover the costs of this action (including reasonable attorneys' fees) and such other relief as the Court deems just and proper.

COUNT VII
DECLARATORY JUDGEMNT
(On Behalf of Plaintiffs and the Nationwide Class)

183. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

184. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

185. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendants are currently maintaining data

security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of his PII will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

186. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiffs' and the Nationwide Class's PII and PHI, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendants' failure to delete PII and PHI it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security number of Plaintiffs.

187. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII of Plaintiffs and the Nationwide Class;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiffs harm.

188. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and

government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendants to:

d. engage third party auditors, consistent with industry standards, to test their systems for weakness and upgrade any such weakness found;

e. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test their systems for security vulnerabilities, consistent with industry standards;

g. implement an education and training program for appropriate employees regarding cybersecurity.

189. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

190. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

191. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Defendants, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

COUNT XIII
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

192. Plaintiffs and the Pennsylvania Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

193. Plaintiffs and Nationwide Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable Private Information.

194. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Nationwide Class Members' Private Information.

195. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Nationwide Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Nationwide Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

196. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Nationwide Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

197. Defendants acquired the monetary benefit and PII and PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

198. If Plaintiffs and Nationwide Class Members knew that Defendants had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendants.

199. Plaintiffs and Nationwide Class Members have no adequate remedy at law.

200. As a direct and proximate result of Defendants' conduct, Plaintiffs and Nationwide Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

201. As a direct and proximate result of Defendants' conduct, Plaintiffs and Nationwide Class Members have suffered and will continue to suffer other forms of injury and/or harm.

202. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Nationwide Class Members, proceeds that they unjustly received from them.

COUNT IX
Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Act Law, 73 P.S. 201-1, *et. seq.*
(On behalf of Plaintiffs and the Pennsylvania Subclass)

203. Plaintiffs and the Pennsylvania Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 97.

204. Plaintiffs the Pennsylvania Subclass members are "persons" within the meaning of 73 P.S. § 201-2(2).

205. Plaintiffs and the Pennsylvania Subclass purchased goods and/or services from Defendants in that they purchased healthcare related good/or services.

206. Defendants engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 P.S. § 201-3, including the following:

207. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 P.S. § 201-2(4)(v));

208. Representing that its goods and services are of a particular standard or quality if they are another (73 P.S. § 201-2(4)(vii));

209. Failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to or after a contract for the purchase of goods or services is made (73 P.S. § 201-2(4)(xiv)); and,

210. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

211. Defendants' unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Pennsylvania Subclass Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures in response to increasing cybersecurity risks in the healthcare sector, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Pennsylvania Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C and § 45, HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Pennsylvania Subclass Members' PII and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Pennsylvania Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. and § 1320d;

f. Failing to timely and adequately notify Plaintiffs and Pennsylvania Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Pennsylvania Subclass Members' PII and PHI; and,

h. Omitting, suppressing, and concealing the material fact that it did not comply with the common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Pennsylvania Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. and § 45, HIPAA, 42 U.S.C. § 1320d.

212. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Pennsylvania Subclass Members,

about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII and PHI.

213. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Pennsylvania Subclass Members, leading them to believe for several months that their PII and PHI was secure and that they did not need to take actions to secure their data.

214. Defendants intended to mislead Plaintiffs and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

215. Had Defendants disclosed to Plaintiffs and Pennsylvania Subclass Members that their Network systems were not secure and thus vulnerable to attack, Defendants would have been forced to adopt reasonable data security measures and comply with the law. Instead, Plaintiffs and Pennsylvania Subclass Members entrusted Defendants with their sensitive and valuable PII and PHI. Defendants accepted the responsibility of being a steward of this data, while keeping the inadequacy of its security measures secret from the public. Accordingly, because Defendants held itself out as maintaining a secure system and comply with state and federal law as well as industry standards,

216. Plaintiffs and Pennsylvania Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

217. Defendants acted intentionally, knowingly, willfully, wantonly, maliciously, and outrageously to violate Pennsylvania's Unfair Trade Practices and Consumer Protection Law and recklessly disregarded Plaintiffs' and Pennsylvania Subclass Members' rights.

218. As a result of Defendants' above-described conduct, Plaintiffs and Pennsylvania Subclass members have suffered damages from the disclosure of their information to unauthorized individuals.

219. The injury and harm that Plaintiffs and the other Pennsylvania Subclass members suffered was the direct and proximate result of Defendants' violations of the UTPCPL. Plaintiffs and Pennsylvania Subclass members have suffered or will suffer economic damages and other injury and actual harm in the form of, inter alia: a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; improper disclosure of their PII/PHI; breach of the confidentiality of their PII/PHI; deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

220. Plaintiffs, individually and on behalf of the Pennsylvania Subclass, request that this Court enter such orders or judgments as may be necessary to enjoin Defendants from continuing its unfair and deceptive practices.

221. Plaintiffs and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, punitive damages, attorneys' fees or costs, and any additional relief the Court deems necessary or proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the Lancaster Subclass, and the Pennsylvania Subclass and appointing Plaintiffs and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII and PHI of Plaintiffs and Class

Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: May 22, 2023

Respectfully Submitted,

/s/ Ryan D. Maxey
K. CLANCY BOYLAN, ESQ. ID# 314117
2005 Market Street, Suite 350
Philadelphia, PA 19103
(215) 446-9795
(215) 446-9799 (FAX)
cboylan@forthepeople.com

Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
rmaxey@ForThePeople.com

Arthur Stock (PBN 64336)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay Street, Ste. 1100
Knoxville, TN 37929
Tel: (865) 247-0080
Fax: (865) 522-0049
astock@milberg.com

Attorneys for Plaintiffs and the Proposed Class

*admitted *pro hac vice*

CERTIFICATE OF SERVICE

I hereby certify that on May 22, 2023, the foregoing document was filed with the Clerk by using the CM/ECF system, which will send notification to all attorneys of record in this matter.

/s/ Ryan D. Maxey